The enemy within

Sunday, 14 August 2022, 8:43 PM

The enemy within

We tend to think of hacks and breaches being committed by script kiddies, anonymous groups, and criminal gangs to name a few, but according to Harvard Business Review's Marc Van Zadelhoff, inside staff are committing a growing number of attacks regardless of their organisation's size. The IBM Cyber Security Intelligence Index (2016, as cited by Van Zadelhoff, 2022) discovered that 2 in 3 attacks were done by insiders. Interestingly, Malicious intent was the cause of 75% cases whereas only 25% was done accidently or without malice.

Security techniques

The International Organisation for Standards (ISO) has developed a set of standards for computer security; this matured into the ISO 27000 family. It is beyond the scope of this blog to cover all aspects of the ISO 27000 family; nevertheless, below are the top five definitions which I consider everyone should know (Iso.org, 2019)

Access control

Who are you and what do you want? The basic premise of access control is to make sure internal users are authorised and enforce the principle of least privilege to use a certain computer systems and resources (Fortinet, n.d.). These requirements are usually set by IAM administrators and follow the five components:

1. Authentication
2. Authorisation
3. Access
4. Manage
5. Audit

Attack

In cyber security, an attack is a malicious attempt by organisations or individuals to destroy, alter, disable, steal, expose, or tamper with an organisation's data and assets. Two of the most common types are phishing and malware. For example, a staff member clicking on an email link that has been loaded with a virus (CISCO, 2019).

Event

An event is defined as a change or occurrence of a particular set of circumstances (Iso.org, 2019). These can range from small to large and occur daily as well as be positive or negative (Miller, 2019). One example of an event is when an internal user incorrectly inputs their password three times and gets locked out.

Monitoring

The protection of the organisation's IT infrastructure, data, and information is vital to ensure the safety and security of all users. Monitoring allows real-time information of the IT systems to be logged, analysed, tracked, detect, and respond to internal threats **events** and **attacks**. Another reason to monitor for governmental and industry standard compliance such as GDPR and ISO 27000 (Sentient Digital, 2020)

Vulnerability

According to owasp.org, (2022), a vulnerability is a weakness in a software application which can be exploited by an inside attacker and causes great harm. Below are a few examples:

Poorly configured code

Data or information not hashed

Out-dated software.

Comments

New comment

Monday, 15 August 2022, 12:22 PM
by Cathryn Peoples

Thanks for your post, Jonny. I consider monitoring to be particularly key, especially given the statistics which you've presented regarding the role played by malice in a system attack. Psychological screening of would-be employees might also be supportive:

Best wishes,

Cathryn

C. Peoples, J. Rafferty, A. Moore and M. Zoualfaghari, "Managing Cybersecurity Events using Service Level Agreements (SLAs) by Profiling the People who Attack," published by Springer in 'Advances in Cybersecurity Management', June 2021

References

CISCO (2019) *Cyber Attack - What Are Common Cyberthreats?* Cisco. Available from: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~how-cyber-attacks-work [Accessed 14 Aug. 2022].

Fortinet. (n.d.) *What Is Access Control? - Network Cybersecurity Systems*. Available from: https://www.fortinet.com/resources/cyberglossary/access-control [Accessed 14 Aug. 2022].

Iso.org. (2019) *ISO/IEC 27000:2018(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed 14 Aug. 2022].

Miller, J. (2019) *Cybersecurity Event / Incident: What's the Difference* | *BitLyft Cybersecurity*. www.bitlyft.com. Available from: https://www.bitlyft.com/resources/cybersecurity-event-vs-incident-whats-the-difference#:~:text=A%20cybersecurity%20event%20is%20a%20change%20in%20the [Accessed 14 Aug. 2022].

Owasp.org. (2022) *Vulnerabilities* | *OWASP*. Available from: https://owasp.org/www-community/vulnerabilities/ [Accessed 14 Aug. 2022].

Sentient Digital, Inc. (2020) *What Is Cyber Monitoring?* Available from: https://sdi.ai/blog/what-is-cyber-monitoring/ [Accessed 14 Aug. 2022].

Van Zadelhoff, M. (2016) *The Biggest Cybersecurity Threats Are Inside Your Company*. Harvard Business Review. Available from: https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company [Accessed 14 Aug. 2022].